UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,104	12/29/2000	Samuel N. Zellner	BS00-027	6281

36192 7590 03/09/2005

CANTOR COLBURN LLP
55 GRIFFIN ROAD SOUTH
BLOOMFIELD, CT 06002

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/750,104	ZELLNER ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42 and 44-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42 and 44-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/18/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

This office action is in response to Applicant's amendment received on October 22, 2004. Claim 43 is cancelled. Claims 45 and 46 are added. Claims 1-42 and 44-46 are pending.

Response to Arguments

Applicant's arguments filed on October 22, 2004 have been fully considered but they are only persuasive to the extent of newly amended claims.

Remarks

In response to amended claims 1, 15, and 36, Applicant argues that none of the prior arts of the record, namely Monroe, Amini, and Vaios teach communication over a secure tunnel as claimed. Applicant's disclosure in the specification with respect to "secure tunnel" is as follows:

"establishing a secured tunnel through firewall by validating the identity of each party in an internet transaction, verifying the integrity of the message or document, ensuring privacy by protecting information from interception during transmission, authorize access, and support for non-repudiation Applicant suggests use of a digital certificate standard such as x.509 standard to replace easily guessed and frequently lost user IDs and passwords (Specification, Page 12, lines 9-22, and Page 13-14, lines 1-22)".

Examiner disagrees and responds that not only Monroe suggests that firewalls may be implemented to protect access (Col. 18, lines 4-26) but also Amini discloses improved levels of network security that instead of relying solely on user IDs and passwords in conventional on-site systems implements x.509 certificates and SSL communication sessions. The client certificate enables client workstation 322 and off-site server 332 to authenticate each other (i.e., validating the identity of each party in an internet transaction, verifying the integrity of the message or document) and to negotiate cryptographic keys to be used in a secure socket layer (SSL) communication session (i.e., ensuring privacy by protecting information from interception during transmission/establishing a secured tunnel for transmission of information)(Col. 6, lines 13-34).

As disclosed in Amini's disclosure, x.509 certificates and SSL communication are described in greater detail in W. Stallings, Cryptography and Network Security: Principles and Practice, Second Edition, 1999. Also, Examiner brings in a new reference, namely Reid, (U.S. Patent No. 6,131,120), which expressly discloses "secure tunnel" in an analogous art using x.509 standard and SSL communication.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-12, 15-22, 25-26, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe, (U.S. Patent No. 6,545,601 and Monroe hereinafter), in view of Amini et al., (U.S. Patent No. 6,698,021 and Amini hereinafter), in further view of Reid, (U.S. Patent No. 6,131,120 and Reid hereinafter).

Regarding claim 1, Monroe discloses a system for controlling devices at a location by an outside entity, the system comprising:

(a) at least one device installed at the location (Col. 12, lines 6-67 and Col. 13, lines 1-9);

(b) an internal computer system in communication with the device, wherein the internal computer system is adapted to control the device (Col. 13, lines 55-67 and Col. 14, lines 1-9);

wherein when a triggering event is detected at the location, one of the internal computer system and the outside entity initiates a communication session between the internal computer system and the outside entity (i.e., implementing firewalls has been suggested)(Col. 5, lines 17-50 and Col. 18, lines 4-26).

Although Monroe discloses firewalls may be implemented to protect access (Col. 18, lines 4-26), Monroe does not expressly disclose a firewall to verify identity information associated with the outside entity.

However, Amini discloses

(c) a firewall in communication with the internal computer system, wherein the firewall is adapted to verify identity information associated with the outside entity,

wherein the outside entity provides identity information to the firewall, and wherein the firewall allows the outside entity to control the device through the internal computer system if the firewall recognizes the identity information (Col. 6, lines 12-34).

While Monroe and Amini substantially disclose the claimed invention, they fail to expressly disclose that the communication is through "secure tunnels".

However, Reid in an analogous art discloses an equivalent communication system through "secure tunnels" (Col. 9, lines 42-67 and Col. 10, lines 1-32).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Monroe to include a firewall to verify identity information associated with the outside entity as disclosed by Amini and to include a communication system through a "secure tunnel" as disclosed by Reid. This modification would have been obvious because one of ordinary skill in the art would have been motivated by suggestions of Amini and Reid to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34), and to define enhanced security beyond the server-based security (Reid, Col. 7, lines 7-45).

Regarding claim 15, Monroe discloses a method for controlling devices at a location by an outside entity, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location (Col. 12, lines 6-67 and Col. 13, lines 1-9);

(b) requesting the outside entity to control the at least one device, and (c) establishing a communication session between the outside entity and the internal computer system (i.e., implementing firewalls has been suggested)(Col. 5, lines 17-50 and Col. 13, lines 55-67 and Col. 14, lines 1-9 and Col. 18, lines 4-26).

Although Monroe discloses firewalls may be implemented to protect access (Col. 18, lines 4-26), Monroe does not expressly disclose authenticating the identity of the outside entity, and (e) allowing the outside entity to control the at least one device through the internal computer system.

However, Amini discloses

(d) authenticating the identity of the outside entity, and (e) allowing the outside entity to control the at least one device through the secure tunnel (Col. 6, lines 12-34).

While Monroe and Amini substantially disclose the claimed invention, they fail to expressly disclose that the communication is through "secure tunnels".

However, Reid in an analogous art discloses an equivalent communication system through "secure tunnels" (Col. 9, lines 42-67 and Col. 10, lines 1-32).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Monroe to include authenticating the identity of the outside entity, and allowing the outside entity to control the at least one device through the secure tunnel as disclosed by Amini and to include a communication system through a "secure tunnel" as disclosed by Reid. This modification would have been obvious because one of ordinary skill in the art would have been motivated by suggestions of Amini and Reid to provide for an increased

confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34), and to define enhanced security beyond the server-based security (Reid, Col. 7, lines 7-45).

Regarding claim 2, Monroe discloses wherein control of the communication session rests exclusively with the outside entity (i.e., ground station remotely monitors and controls the commercial transport onboard systems)(Col. 3, lines 25-55).

Regarding claims 3 and 19, Monroe discloses wherein the outside entity is an emergency response unit (Col. 7, lines 10-37).

Regarding claim 4, Monroe discloses wherein the emergency response unit is a public safety answering point (i.e., the ground station may also send operational commands to the various monitoring systems both onboard the transport and ground mounted, such as camera tilt, pan and zoom and sensor activation. Other command signals such as "lock-on" a specific condition or transport, sensor download, activation such as "lights-on" or alarm, e.g., siren, activation and the like)(Col. 7, lines 10-37).

Regarding claims 5 and 20, Monroe discloses wherein the outside entity is a private security firm (Col. 7, lines 10-37).

Regarding claim 6, Monroe does not expressly disclose wherein the identity information is a password.

However, Amini discloses wherein the identity information is a password (Col. 6, lines 13-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include an identity information such as a password with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 7, Monroe does not expressly disclose wherein the identity information is a digital certificate.

However, Amini discloses wherein the identity information is a digital certificate (i.e., x.509 certificate)(Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include an identity information such as a digital certificate with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 8, Monroe does not expressly disclose wherein the digital certificate is issued and authenticated by a certificate authority.

However, Amini discloses wherein the digital certificate is issued and authenticated by a certificate authority (Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the digital certificate is issued and authenticated by a certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 9, Monroe discloses further comprising a sensing apparatus in communication with the internal computer system, wherein the triggering event is detected by the sensing apparatus (Col. 6, lines 30-52).

Regarding claims 10 and 17, Monroe discloses wherein the at least one device is an observation device (i.e., camera)(Col. 4, lines 47-65).

Regarding claims 11 and 18, Monroe discloses wherein the at least one device is an emergency response device (i.e., sensors are triggered/activated and only signals generated thereby are transmitted to the security station)(Col. 6, lines 30-53).

Regarding claims 12 and 22, Monroe discloses wherein the internal computer system is a local area network (Col. 3, lines 55-67).

Regarding claim 16, Monroe discloses wherein only the outside entity can terminate the communication session (i.e., ground station remotely monitors and controls the commercial transport onboard systems)(Col. 3, lines 25-55).

Regarding claim 21, Monroe discloses wherein the outside entity is a healthcare provider (Col. 7, lines 10-37).

Regarding claim 25 and 26, Monroe discloses further comprising the step of transferring the communication session from the outside entity to a third party and wherein the third party is an emergency response unit (Col. 7, lines 10-37).

Regarding claim 29, Monroe does not expressly disclose wherein the identity of the outside entity is authenticated by a certificate authority.

However, Amini discloses wherein the identity of the outside entity is authenticated by a certificate authority (Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the identity of the outside entity is authenticated by a certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 30, Monroe does not expressly disclose wherein the identity of the outside entity is authenticated by the internal computer system based on a password provided by the outside entity.

However, Amini discloses wherein the identity of the outside entity is authenticated by the internal computer system based on a password provided by the outside entity (Col. 6, lines 13-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the identity of the outside entity is authenticated by the internal computer system based on a password provided by the outside entity with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Claims 13-14, 27-28, 31-42, 44, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe, (U.S. Patent No. 6,545,601 and Monroe hereinafter), and Amini et al., (U.S. Patent No. 6,698,021 and Amini hereinafter), in view of Reid, (U.S. Patent No. 6,131,120 and Reid hereinafter), in further view of Vaios, (U.S. Patent No. 6,271,752 and Vaios hereinafter).

Teachings of Monroe, Amini, and Reid, with respect to claims 1 and 15 have been discussed previously.

Regarding claims 13-14, and 27-28, Monroe or Amini does not expressly disclose wherein the communication session uses transmission control protocol and/or digital communications protocol.

However, Vaios discloses wherein the communication session uses transmission control protocol and or digital communications protocol (Col. 6, lines 54-67 and Col. 7, lines 1-22).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Monroe and Amini with the teachings of Vaios because it would allow to include wherein the communication session uses transmission control protocol and/or digital communications protocol with the motivation to provide for an inexpensive multi-access remote system that enables individuals to access remotely a security surveillance or other video system area and appropriately monitor and operate this area as desired (Vaios, Col. 1, lines 60-67).

Regarding claim 31, Monroe discloses a system for enabling an outside entity to control devices at a location, the system comprising:

(a) an internal computer system associated with the location (Col. 12, lines 6-67 and Col. 13, lines 1-9);

(b) a sensing apparatus associated with the internal computer system, wherein the sensing apparatus can detect a triggering event at the location wherein when the

sensing apparatus detects the triggering event the internal computer system establishes a communication session with the outside entity via an external computer network (Col. 5, lines 17-50).

Although Monroe discloses firewalls may be implemented to protect access (Col. 18, lines 4-26), Monroe does not expressly disclose a firewall to verify identity information associated with the outside entity.

However, Amini discloses

(c) a firewall in communication with the internal computer system, wherein the firewall is adapted to verify identity information associated with the outside entity, and (d) a device associated with the internal computer system, wherein the device can be controlled by the outside entity via the internal computer system, wherein the outside entity provides identity information to the internal computer system, wherein the firewall creates a secured tunnel for the outside entity to access the internal computer system, wherein the outside entity uses information retrieved from a database to control the device during the communication session (Col. 6, lines 12-34).

Monroe or Amini does not expressly disclose wherein only the outside entity can terminate the communication session.

However, Vaios discloses wherein only the outside entity can terminate the communication session (Col. 8, lines 35-67 and Col. 9, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include a firewall to verify identity information

associated with the outside entity with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34), and to modify the combined teachings of Monroe and Amini with the teachings of Vaios because it would allow to include wherein only the outside entity can terminate the communication session with the motivation to provide for an inexpensive multi-access remote system that enables individuals to access remotely a security surveillance or other video system area and appropriately monitor and operate this area as desired (Vaios, Col. 1, lines 60-67).

Regarding claim 32, Monroe does not expressly disclose wherein the identity information is a password.

However, Amini discloses wherein the identity information is a password (Col. 6, lines 13-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include an identity information such as a password with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 33, Monroe does not expressly disclose wherein the identity information is a digital certificate.

However, Amini discloses wherein the identity information is a digital certificate (i.e., x.509 certificate)(Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include an identity information such as a digital certificate with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 34, Monroe does not expressly disclose wherein the digital certificate is issued and authenticated by a certificate authority.

However, Amini discloses wherein the digital certificate is issued and authenticated by a certificate authority (Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the digital certificate is issued and authenticated by a certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 35, Monroe does not expressly disclose wherein the external computer network is the Internet.

However, Amini discloses wherein the external computer network is the Internet (Col. 13, lines 40-51).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the external computer network is the Internet with the motivation to facilitate connection between client workstations and off-site server (Amini, Col. 13, lines 40-51).

Regarding claims 36 and 46, Monroe discloses a method for enabling an outside entity to control devices at a location, the method comprising the steps o£

(a) associating at least one device with an internal computer system at the location (Col. 12, lines 6-67 and Col. 13, lines 1-9);

(b) reporting a triggering event associated with the location to the outside entity, and (c) initiating a communication session between the internal computer system and the outside entity through an external computer network, wherein the communication session is initiated by the internal computer network (Col. 5, lines 17-50 and Col. 13, lines 55-67 and Col. 14, lines 1-9).

Although Monroe discloses firewalls may be implemented to protect access (Col. 18, lines 4-26), Monroe does not expressly disclose verifying identity information provided by the outside entity, and allowing the outside entity to control the device during the communication session.

However, Amini discloses

(d) verifying identity information provided by the outside entity, and (e) allowing the outside entity to control the device during the communication session (Col. 6, lines 12-34).

While Monroe and Amini substantially disclose the claimed invention, they fail to expressly disclose that the communication is through "secure tunnels".

However, Reid in an analogous art discloses an equivalent communication system through "secure tunnels" (Col. 9, lines 42-67 and Col. 10, lines 1-32).

Monroe, Amini, or Reid does not expressly disclose wherein only the outside entity can terminate the communication session.

However, Vaios discloses wherein only the outside entity can terminate the communication session (Col. 8, lines 35-67 and Col. 9, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Monroe to include a firewall to verify identity information associated with the outside entity as disclosed by Amini and to include a communication system through a "secure tunnel" as disclosed by Reid. This modification would have been obvious because one of ordinary skill in the art would have been motivated by suggestions of Amini and Reid to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34), and to define enhanced security beyond the server-based security (Reid, Col. 7, lines 7-45).

Also, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Monroe, Amini, and Reid

to include wherein only the outside entity can terminate the communication session as disclosed by Vaios. This modification would have been obvious because one of ordinary skill in the art would have been motivated by suggestions of Vaios to provide for an inexpensive multi-access remote system that enables individuals to access remotely a security surveillance or other video system area and appropriately monitor and operate this area as desired (Vaios, Col. 1, lines 60-67).

Regarding claim 37, Monroe does not expressly disclose wherein the identity information is a password issued to the outside entity by the internal computer system.

However, Amini discloses wherein the identity information is a password issued to the outside entity by the internal computer system (Col. 6, lines 13-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include an identity information such as a password with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 38, Monroe discloses wherein the identity information is a digital certificate issued to the outside entity by a certificate authority.

However, Amini discloses wherein the identity information is a digital certificate issued to the outside entity by a certificate authority (Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the identity information is a digital certificate issued to the outside entity by a certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 39, Monroe does not expressly disclose wherein the step of verifying the identity information of the outside entity is performed by the certificate authority.

However, Amini discloses wherein the step of verifying the identity information of the outside entity is performed by the certificate authority (Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the step of verifying the identity information of the outside entity is performed by the certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 40, Monroe does not expressly disclose further comprising the step of authenticating identity of the internal computer system for the outside entity.

However, Amini discloses further comprising the step of authenticating identity of the internal computer system for the outside entity further comprising the step of authenticating identity of the internal computer system for the outside entity (i.e., the client certificates enable client workstation 322 and off-site server 332 to authenticate each other and to negotiate cryptographic keys to be used in a secure socket layer (SSL) communication session)(Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include the step of authenticating identity of the internal computer system for the outside entity further comprising the step of authenticating identity of the internal computer system for the outside entity with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 41, Monroe discloses a method for enabling an outside entity to handle a situation at a location, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location (Col. 12, lines 6-67 and Col. 13, lines 1-9);

(b) reporting a triggering event associated with the situation at the location to the outside entity, and (c) initiating a communication session between the internal computer system and the outside entity through an external computer network (Col. 5, lines 17-50 and Col. 13, lines 55-67 and Col. 14, lines 1-9).

Although Monroe discloses firewalls may be implemented to protect access (Col. 18, lines 4-26), Monroe does not expressly disclose providing first and second identity information associated with the internal computer system to the outside entity and authenticating both the first identity information and the second identity information.

However, Amini discloses

(d) providing a first identity information associated with the internal computer system to the outside entity, (e) providing a second identity information associated with the outside entity to the internal computer system, (f) authenticating both the first identity information and the second identity information: (g) establishing a secured tunnel through a firewall associated with the internal computer system if both the first identity information and the second identity information are authenticated, and (h) allowing the outside entity to control the device to handle the situation during the communication session (Col. 6, lines 12-34).

Monroe, Amini, or Reid does not expressly disclose wherein only the outside entity can terminate the communication session.

However, Vaios discloses wherein only the outside entity can terminate the communication session (Col. 8, lines 35-67 and Col. 9, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include a firewall to verify identity information associated with the outside entity with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation

(Amini, Col. 6, lines 12-34), and to modify the combined teachings of Monroe and Amini with the teachings of Vaios because it would allow to include wherein only the outside entity can terminate the communication session with the motivation to provide for an inexpensive multi-access remote system that enables individuals to access remotely a security surveillance or other video system area and appropriately monitor and operate this area as desired (Vaios, Col. 1, lines 60-67).

Regarding claim 42, Monroe does not expressly disclose wherein the first identity information is a first digital certificate issued to the internal computer system by a certificate authority.

However, Amini discloses wherein the first identity information is a first digital certificate issued to the internal computer system by a certificate authority (i.e., the client certificates enable client workstation 322 and off-site server 332 to authenticate each other and to negotiate cryptographic keys to be used in a secure socket layer (SSL) communication session)(Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the step of verifying the identity information of the outside entity is performed by the certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Regarding claim 44, Monroe does not expressly disclose wherein the step of authenticating both the first identity information and the second identity information is performed by a certificate authority.

However, Amini discloses wherein the step of authenticating both the first identity information and the second identity information is performed by a certificate authority (i.e., the client certificates enable client workstation 322 and off-site server 332 to authenticate each other and to negotiate cryptographic keys to be used in a secure socket layer (SSL) communication session)(Col. 6, lines 12-34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Monroe with the teachings of Amini because it would allow to include wherein the step of verifying the identity information of the outside entity is performed by the certificate authority with the motivation to provide for an increased confidentiality of video images obtained by the surveillance and monitoring operation (Amini, Col. 6, lines 12-34).

Claims 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe, (U.S. Patent No. 6,545,601 and Monroe hereinafter), Amini et al., (U.S. Patent No. 6,698,021 and Amini hereinafter), and Reid, (U.S. Patent No. 6,131,120 and Reid hereinafter), in view of Engelhorn et al., (U.S. Patent No. 6,317,042 and Engelhorn hereinafter).

Teachings of Monroe, Amini, and Reid, with respect to claim 15, have been discussed previously.

Regarding claims 23 and 24, Monroe or Amini does not expressly disclose wherein the internal computer system is Bluetooth compatible and at least one device is Bluetooth-enabled.

However, discloses wherein the internal computer system is Bluetooth compatible and at least one device is Bluetooth-enabled (Col. 3, lines 25-67 and Col. 4, lines 1-44).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Monroe, Amini, and Reid to include wherein the internal computer system is Bluetooth compatible and at least one device is Bluetooth-enabled as disclosed by Engelhorn. This modification would have been obvious because one of ordinary skill in the art would have been motivated by suggestions of Engelhorn to provide for n emergency announcement system that displays an escape route for occupants of a building (Engelhorn, Col. 1, lines 1-20).

Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe, (U.S. Patent No. 6,545,601 and Monroe hereinafter), Amini et al., (U.S. Patent No. 6,698,021 and Amini hereinafter), Reid, (U.S. Patent No. 6,131,120 and Reid

hereinafter), and Vaios, (U.S. Patent No. 6,271,752 and Vaios hereinafter), in view of Kung et al., (U.S. Patent No. 6,252,952 and Kung hereinafter).

Teachings of Monroe, Amini, Reid, and Vaios, with respect to claim 41, have been discussed previously.

Regarding claim 45, Monroe, Amini, Reid, or Vaios does not expressly disclose wherein the triggering event is a call from a voice-over-Internet-protocol (VOIP) device.

However, Kung discloses wherein the triggering event is a call from a voice-over-Internet-protocol (VOIP) device (Col. 9, lines 39-67 and Col. 10, lines 1-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of remote controlling system of Monroe, Amini, Reid, and Vaios by including a call from a voice-over-Internet-protocol (VOIP) device as disclosed by Kung. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Kung to provide for a mechanism to start and/or end the billing procedure (Kung, Col. 30, lines 1-20).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

http://java.sun.com/j2se/1.5.0/docs/guide/security/cert3.html

Reid, (U.S. Patent No. 6,131,120).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
March 1, 2005

Gregory J. Lamarre
Primary Examiner